THE IMPACT OF TECHNOLOGY ON THE COURTS

Thomas Sadaka
Seiden Alder Matthewman & Bloch
Boca Raton, Coral Springs, Miami & Orlando

Objectives

To be able to describe

- Evolving uses of computer technology
- Increasing ubiquity of digital devices
- Types and sources of digital data
- The massive collection of digital information
- Challenges of applying the Fourth Amendment
- Proliferating “surveillance” tools and concerns
- Relevance for all lawyers & judges

Advancing Technology

Computers

Computer & Internet Uses

- Productivity
- Information
- Infrastructure controls
- Communication / social interaction
- Publishing / broadcasting
- Shopping / commerce
- Entertainment / recreation
- Surveillance / law enforcement

The “Internet”

- Web & Web 2.0
- E-mail & Web-based e-mail
- Chat rooms / IRC
- Instant messaging
- Telephone calls – Voice over IP
- Newsgroups, e-groups, mailing lists
- FTP sites and bulletin boards
- Peer-to-peer networks
- Role playing games, “virtual worlds”
- Remote data storage & processing

Computer Uses, Roles

- Computers and networks can be
  - **Targets**
  - **Tools**
  - **Containers** of evidence
  - Combinations

Digital Data – Evidence

- **User-created**
  - Text (documents, e-mail, chats, instant messages)
  - Address books
  - Bookmarks
  - Databases
  - Images (photos, drawings, diagrams)
  - Video and sound (films, voice mail, .wav files)
  - Web pages
  - Hidden files

Digital Data – Evidence

- **Computer-created**
  - Email headers
  - Metadata
  - Activity logs
  - Browser cache, history, cookies
  - Backup and registry files
  - Configuration files
  - Printer spool files
  - Swap files and other “transient” data
  - Surveillance tapes, recordings

Data Generated in 2006*

- 161 billion gigabytes (161 exabytes)
- 12 stacks of books each reaching from the Earth to the Sun
- 3 million times all the books ever written
- Would need more than 2 billion iPods to hold it

*According to report by technology research firm IDC

How Much Data?

- **Byte** (8 bits)
  - 1 byte: A single character
  - 10 bytes: A single word
- **Kilobyte** (1,000 bytes)
  - 1 KB: A paragraph
  - 10 KB: An encyclopedic page
- **Megabyte** (1,000 KB)
  - 1 MB: A small book
  - 2 MB: A high resolution photograph
  - 5 MB: The complete works of Shakespeare

How Much Data?

- **Gigabyte** (1,000 MB)
  - 1 GB: 10 yards of shelved books
  - 50 GB: A floor of books
- **Terabyte** (1,000 GB)
  - 1 TB: 300 hours of video OR 1,000 copies of the Encyclopedia Britannica
  - 10 TB: Printed collection of the Library of Congress
- **Petabyte** (1,000 TB)
  - 1 PB: 20 million four-door filing cabinets full of text
  - 2 PB: All US academic research libraries
- **Exabyte** (1,000 PB)
  - 5 EB: All words ever spoken by humans

Challenges

- Increasing ubiquity and convergence of digital devices
- Increasing data storage capacity
- Shrinking devices and media
- Growing use of solid state devices

Where Digital Evidence Found

- Home computers
- Thumb drives and other external storage
- P2P network share folders
- Office workstations
- Network servers
- Cell phones, PDAs, other portable devices
- Internet & Online Service Providers
- Vehicles
- New and evolving devices

Digital devices

Digital devices

Digital devices

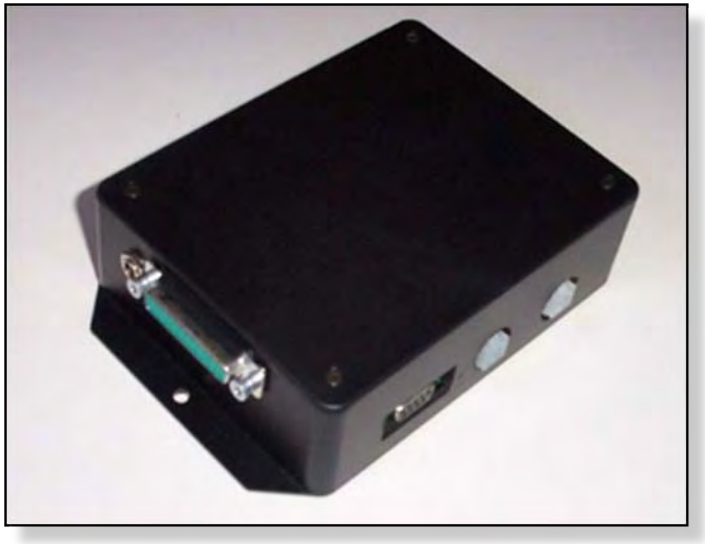
Digital devices

Digital devices

Digital devices

Vehicle “black boxes”

- Event data recorders
- Sensing and diagnostic modules



Digital devices

Digital devices

"Yes, it's self-defrosting. It also does a daily inventory, searches for the best deal and runs over to the store for you."

Fourth Amendment

- Does it apply?
- When does gov't action regarding data amount to a "search" or "seizure"?
- Do users of computers or the Internet have reasonable expectations of privacy?
  - In what information?
  - In which locations or devices?
  - When?
- How is the FA satisfied?

Nature of Computer Searches

- Should computers be treated like “containers”?
- Should computers be treated differently, requiring a “special approach”?
- Are the “rules” different for computers?
  - Should they be?
- Do the rules apply differently depending on the type of digital device or data?

Applying Fourth Amendment

- How is a search for digital data different, if at all, from a document search?
- Is there a constitutional basis for requiring special warrant execution protocols, to delimit search procedures?
- Should amount of personal or intermingled information make a difference?
- What about private searches, and exceptions to the warrant requirement?

Surveillance

- What other laws constrain or authorize real-time or "historical" evidence collection, via interceptions or monitoring or from third parties?
- Are they adequate or appropriate in light of evolving technology?
- Are additional privacy protections needed?
- Must we accept reductions in privacy?

Surveillance?

333 S. John Q. Hammons Pkwy, Springfield, MO 65806 - Google Maps - Mozilla Firefox

File Edit View History Bookmarks Tools Help

333 S. John Q. Hammons Pkwy, S...

Web Images Video News **Maps** Gmail more ▼ Saved Locations | Sign in | Help

Google Maps

e.g., "10 market st, san francisco" or "hotels near lax"

333 S. John Q. Hammons Pkwy, Springfield, MO 65806 Search Maps

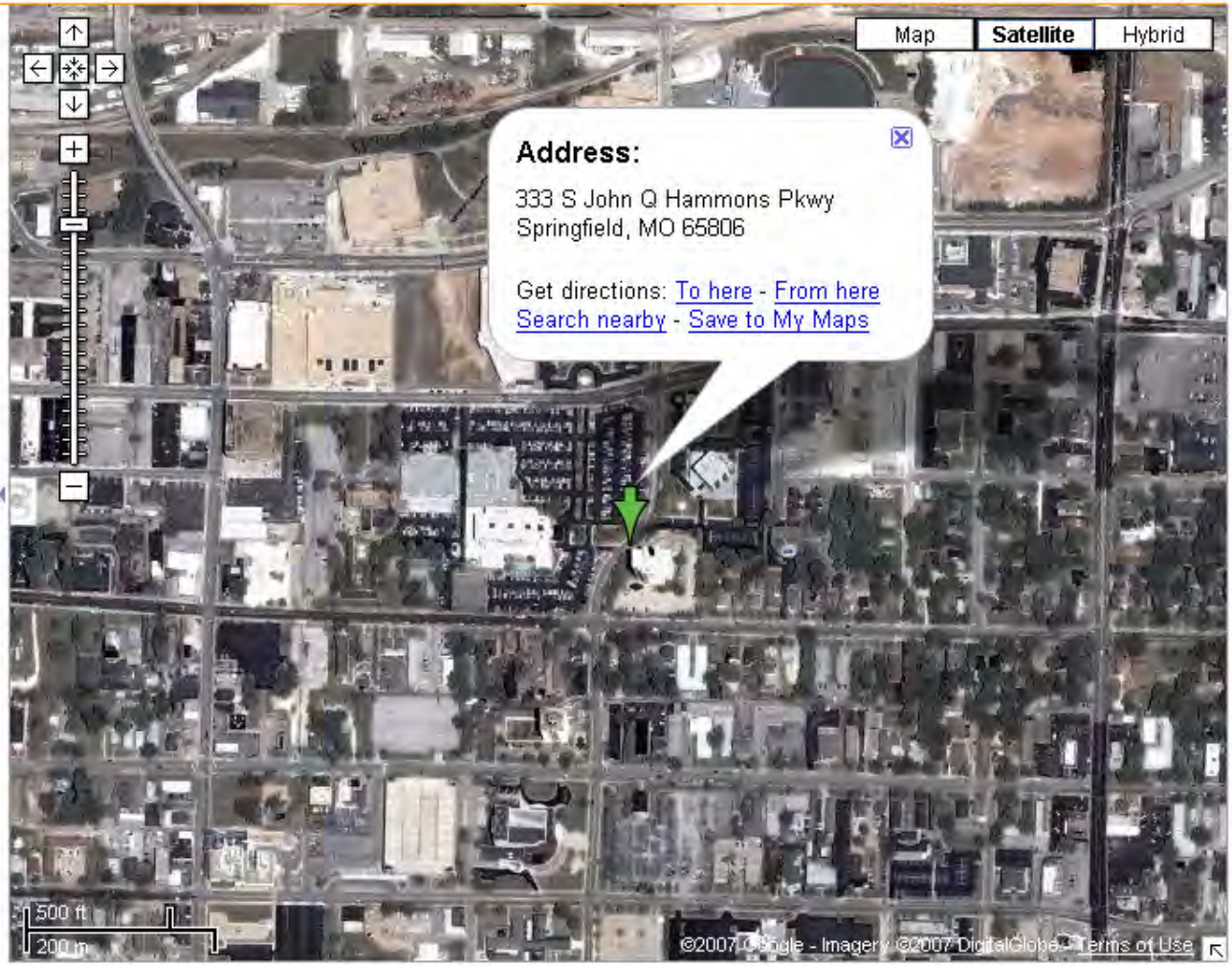
Search the map Find businesses Get directions

Search Results My Maps

Print Send Link to this page

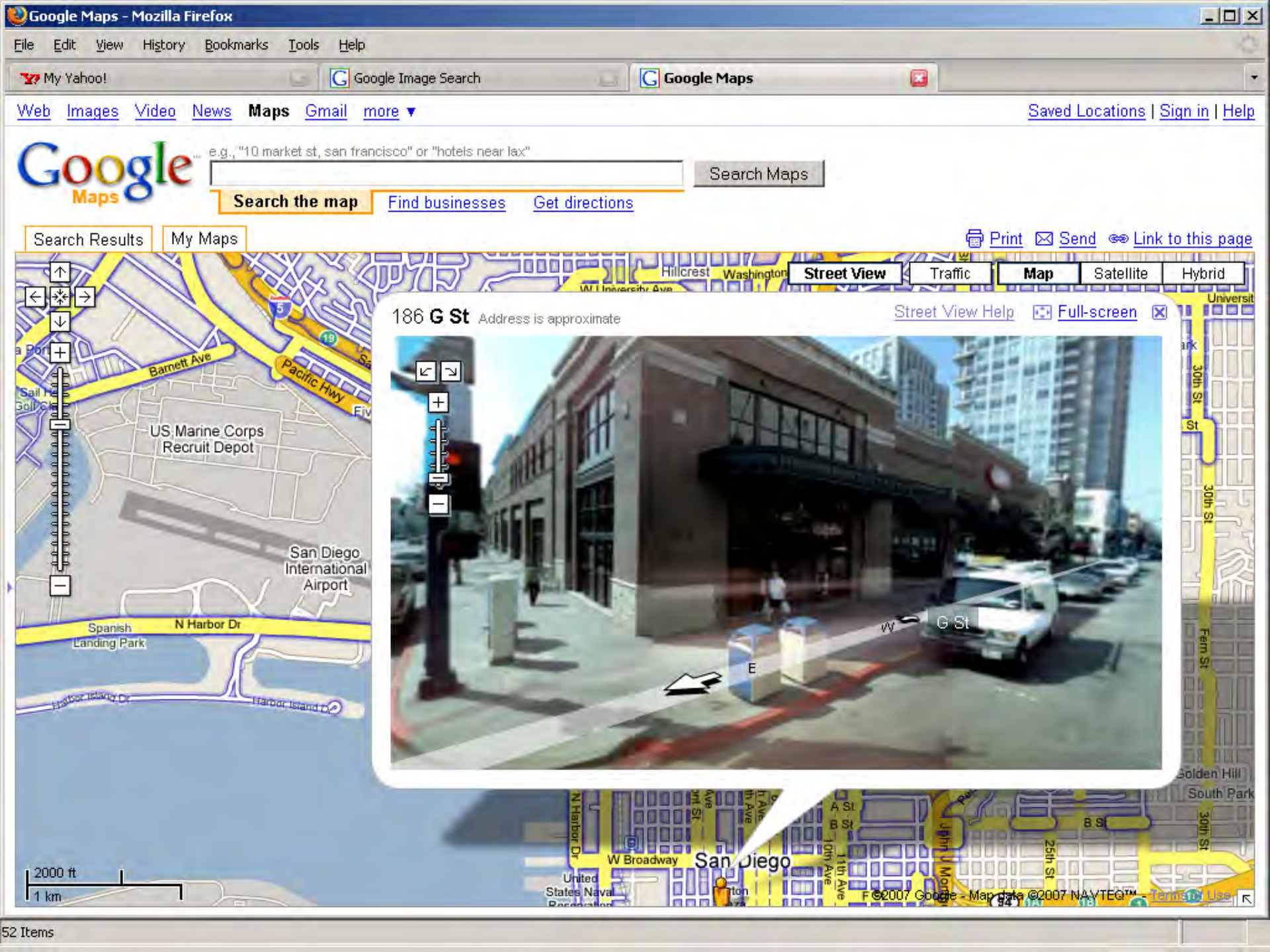
333 S John Q Hammons Pkwy
Springfield, MO 65806

Make this my default location

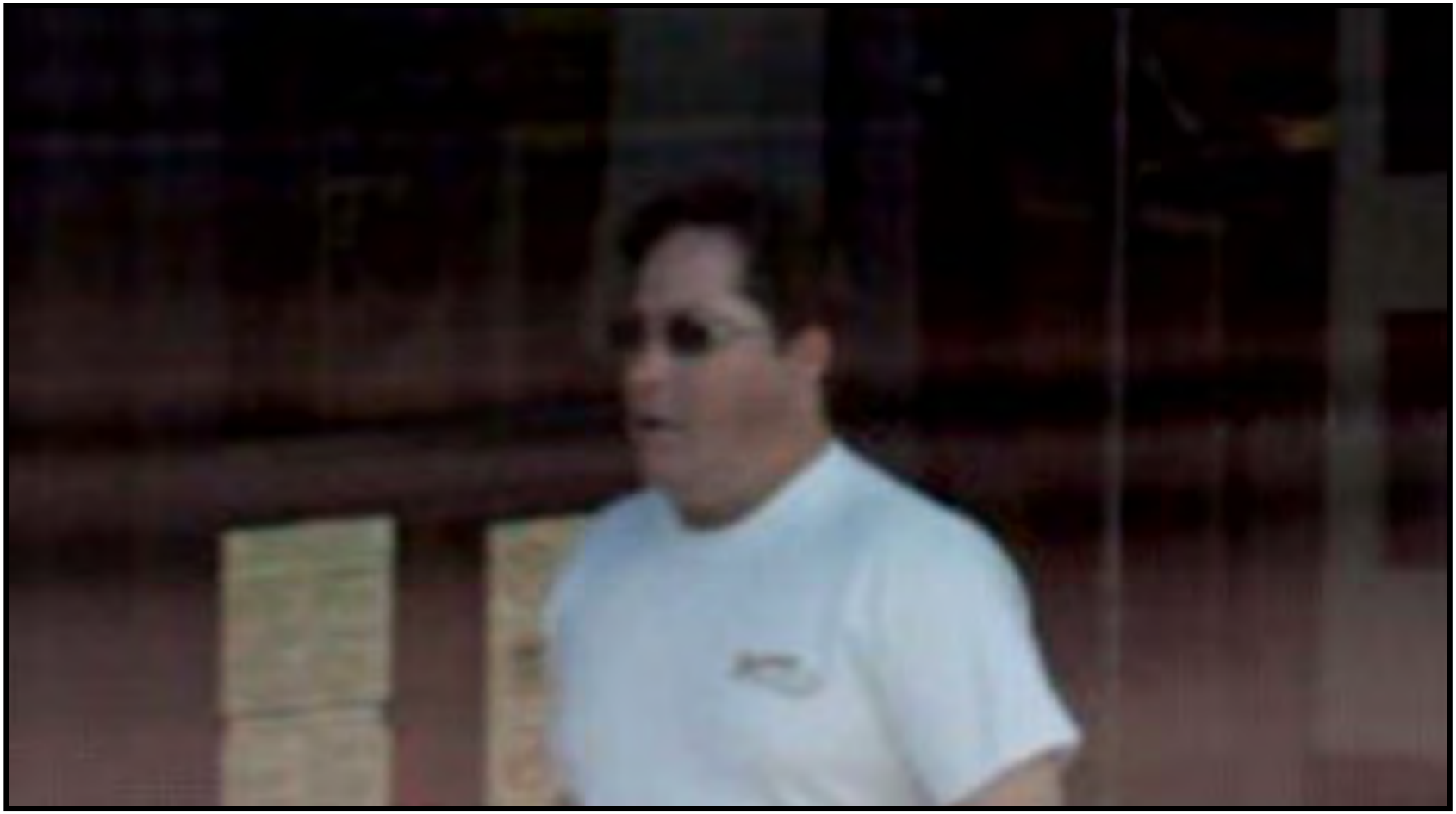


Done


Map
Satellite
Hybrid
100 ft
50 m
©2007 Google - Imagery ©2007 DigitalGlobe - Terms of Use


Google Maps - Mozilla Firefox
File Edit View History Bookmarks Tools Help
My Yahoo!
Google Image Search
Google Maps
Web Images Video News Maps Gmail more ▼
Saved Locations | Sign in | Help
Google Maps
e.g., "10 market st, san francisco" or "hotels near lax"
Search Maps
Search the map
Find businesses
Get directions
Search Results
My Maps
Print
Send
Link to this page
Street View
Traffic
Map
Satellite
Hybrid
186 G St
Address is approximate
Street View Help
Full-screen
G St
E
W
Barnett Ave
Pacific Hwy
US Marine Corps Recruit Depot
San Diego International Airport
Spanish Landing Park
N Harbor Dr
Harbor Island Dr
Hillcrest
Washington
30th St
Fern St
Golden Hill
South Park
W Broadway
San Diego
United States Naval
2000 ft
1 km
©2007 Google - Map data ©2007 NAVTEQ™ - Terms of Use
52 Items

Recognizable?



Surveillance cameras

Intra-family "surveillance"?

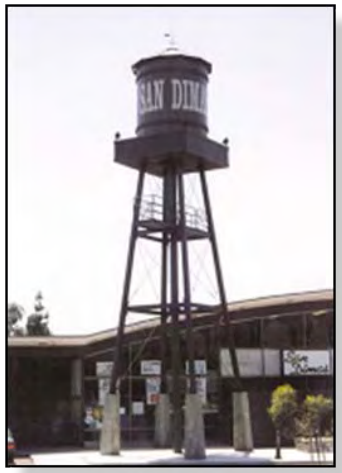
Divorce Court Properly Excluded Online Communications Intercepted by Wife

A woman who installed spyware on her husband's computer in order to monitor his online conversations and e-mails with another woman "intercepted" electronic communications in violation of state law, Florida's Fifth District Court of Appeal held Feb. 11 (*O'Brien v. O'Brien*, 2005 WL 322367 (Fla. Dist. Ct. App., decided February 11, 2005).

The court thus rejected Beverly Ann O'Brien's contention that the judge in the couple's divorce proceeding erred in refusing to admit evidence of her husband's computer activities obtained via the spyware.

Although the court found that the state electronic privacy statute did not bar admission of such intercepted electronic communications, it concluded that because the wife acquired the evidence unlawfully, the judge acted within his discretion in excluding it.

Surveillance tools?



Surveillance tool?

RFID – Privacy implications?

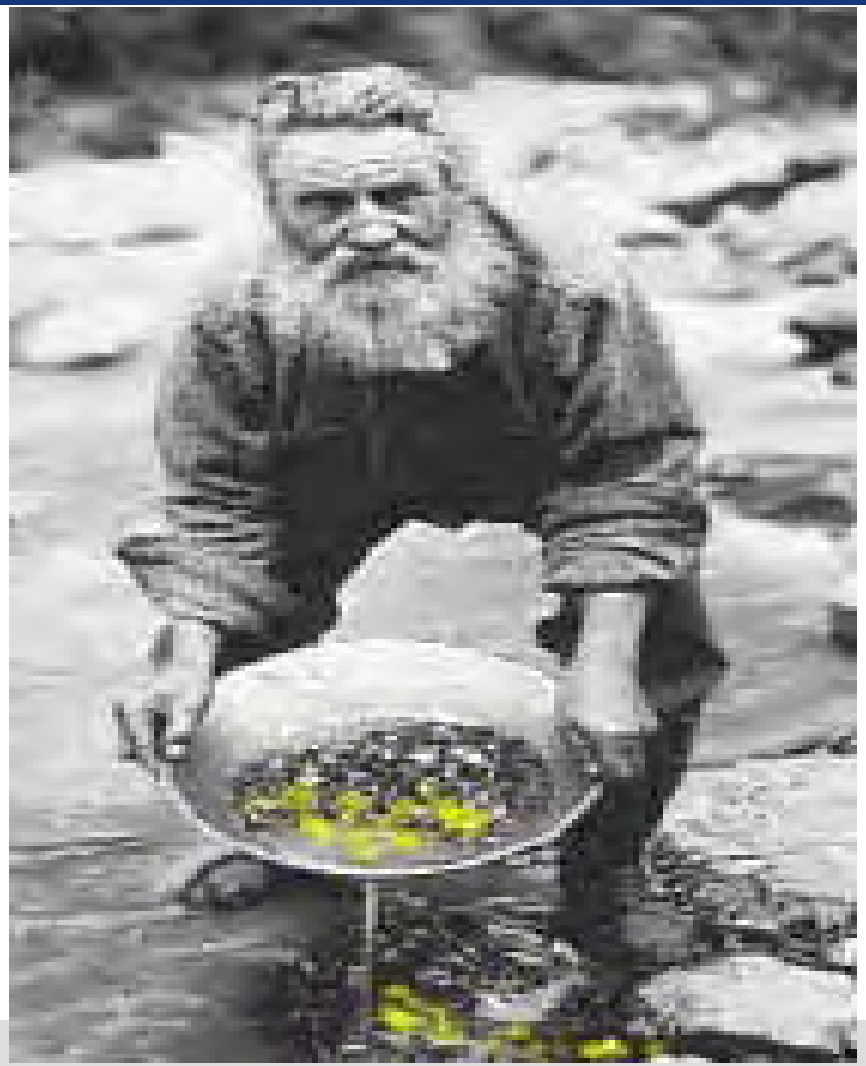
Questions?

- Thomas A. Sadaka
- Seiden Alder Matthewman & Bloch
- Celebration Corporate Center
- 1420 Celebration Blvd, Suite 201
- Celebration, FL 34741
- 407-566-2110
- tsadaka@seidenlaw.com

Introduction to Forensics Civil and Criminal Implications

Presented By
Thomas A. Sadaka

Computer Forensics



COMPUTER FORENSICS

The use of sophisticated technological tools and procedures to preserve, identify, extract, and document computer evidence

Why so Important

- ✓ **The goal of the computer forensic process is to reliably determine if evidence exists and, if so, to be able to use that evidence in some subsequent action**
- ✓ **Without proper procedures and best practices the usefulness of the information obtained is compromised**
- ✓ **Must have policies and procedures insuring**
  - Proper seizure
  - Proper storage
  - Proper acquisition
  - Proper analysis
  - Competent testimony

Proper Seizure – “Crime Scene”

“Crime Scene”

Electronic Data (crime scene) Locations

- PC– not just workstations…
- Network drives
- Routers
- Backup tapes
- Old computers
- Third party vendors
- The Internet and intranet
- Log files, access control lists, passwords

Chain of Custody Issues

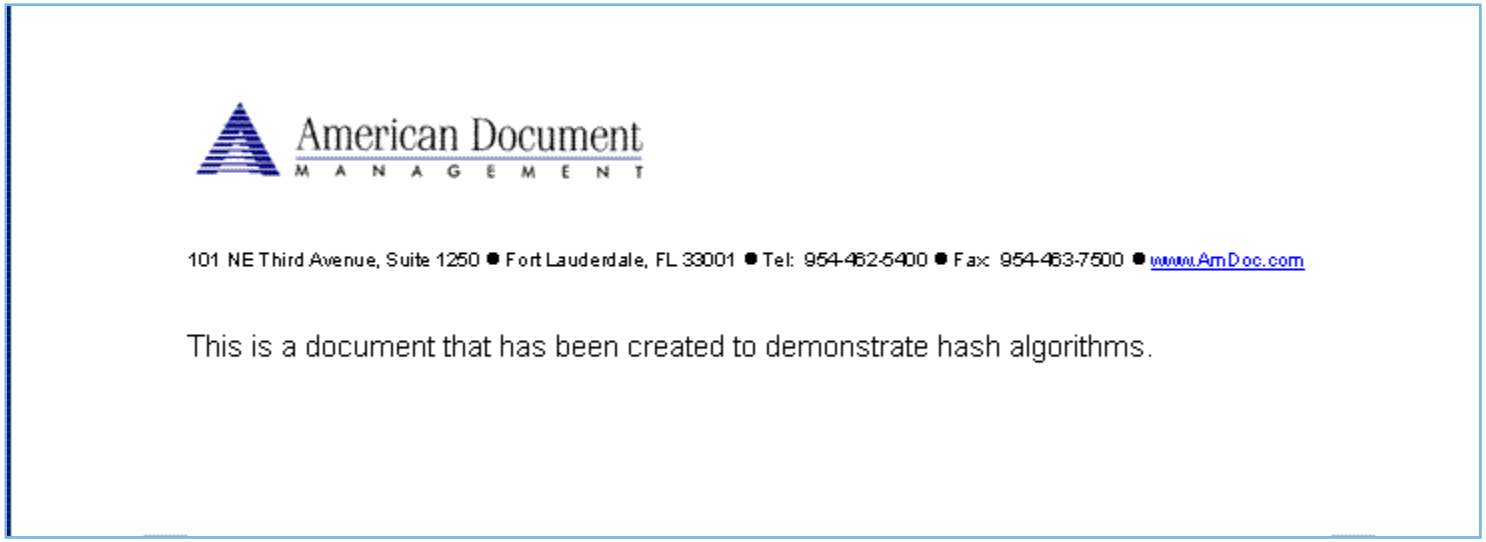
- ✓ **Physical Items – the seizure of the physical items should conform to best practices for handling of computers or other repositories of digital evidence**
- ✓ **Data Acquisition – the acquisition of data from the seized physical item should also conform to best practices – if so, concerns about the chain of custody of the data contained in the forensic image become moot.**

Proper Seizure – How Do We Know

"HASH"

- **Digital "fingerprint" of data**
  - Any change changes hash
  - Including formatting change
- **MD5 Hash**
  - Message Digest algorithm #5 (128 bit)
  - 1991 – Ronald Rivest, MIT
  - "Flaws" – security, not document
- **SHA1 Hash**
  - Secure Hash Algorithm (160 bit)
  - SHA0 - 1993 – Nat'l Institute of Standards
  - 5 algorithms for NSA security

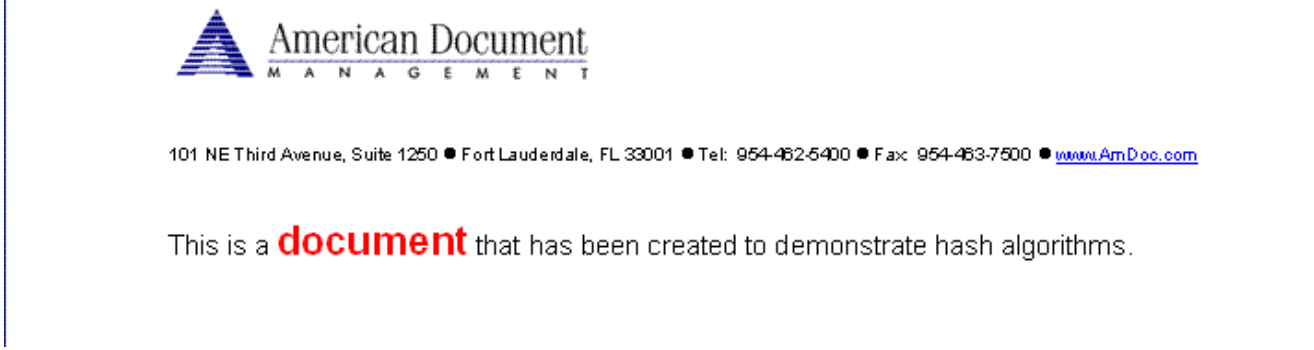
Examples



- ✓ **MD5:**
- ✓ 2F9E032BB67617AC098FC0992E09C37F

- ✓ **SHA1:**
- ✓ 83A970AB80F3A2E25C2DC9C054A4DD0AA0A4FE37

Example



American Document
MANAGEMENT

101 NE Third Avenue, Suite 1250 ● Fort Lauderdale, FL 33001 ● Tel: 954-462-5400 ● Fax: 954-463-7500 ● www.AmDoc.com

This is a **document** that has been created to demonstrate hash algorithms.

- ✓ **MD5:**
- ✓ 2F9E032BB67617AC098FC0992E09C37F (Original)
- ✓ 3F95449E532AA13B3BFDC2FAA826A234 (New)
- ✓ **SHA1:**
- ✓ 83A970AB80F3A2E25C2DC9C054A4DD0AA0A4FE37 (Original)
- ✓ 08386D11FDA3AED071D0F4273A65F569C255C2F3 (New)

Questions To Answer

Forensics capture warranted?

- ✓ Context important?
- ✓ Deleted files important?
- ✓ Tracking access important?
- ✓ Criminal case?

Devices to be examined?

- ✓ Hard drives
- ✓ Cell phones
- ✓ PDAs
- ✓ Voice mail
- ✓ Cameras
- ✓ GPS tracking devices?

What is forensic duplication?

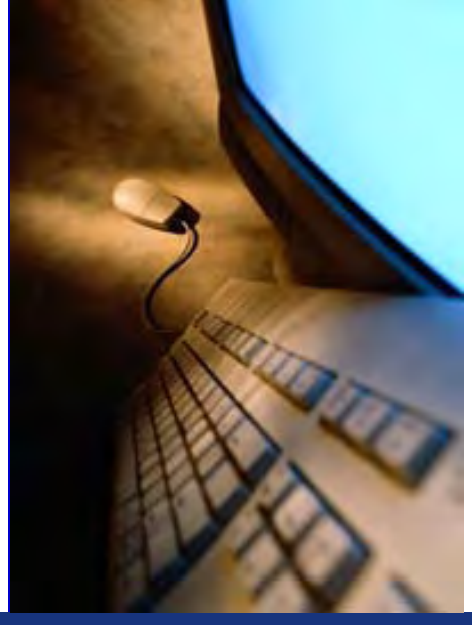
A *forensic duplicate* or an image is an exact “bit for bit, sector by sector” copy of all user accessible data objects from a suspects drive onto another hard drive or some form of digital media from which the original drives contents can be recreated if so desired.

Data Integrity

- ✓ **Must be able to demonstrate in court that the information obtained from the media is a true and accurate representation of the information originally contained in the media**
  - Issues surrounding Chain of Custody. There are two chains to consider:
    - Physical
    - acquisition

Data Integrity

- ✓ **Every time a hard drive is handled, you run the risk of damaging the electronic evidence.**
- ✓ **Protect Media As Evidence**
  - Turning On A Windows-Based Computer Changes The Contents
  - Backing Up Data Can Change Its Contents
  - Opening a file changes its content

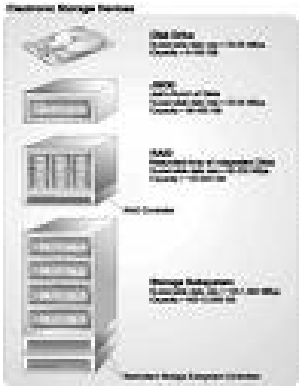


Evidence

LOCATION OF EVIDENCE

Where do you find electronic evidence?

Electronic Storage Devices

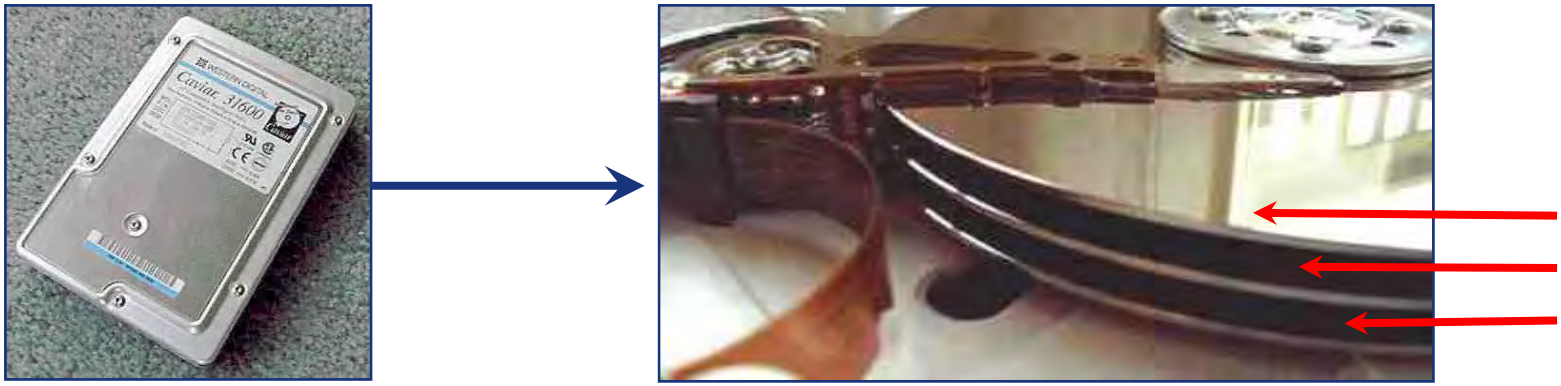


Hard Drives

All computers have one or more hard drives

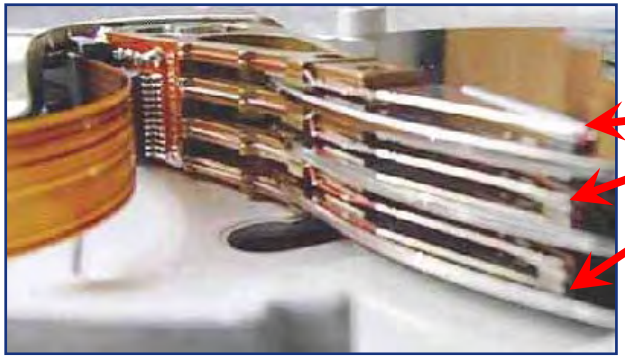
Photos from www.howstuffworks.com

Hard drives have multiple platters



Photos from www.howstuffworks.com

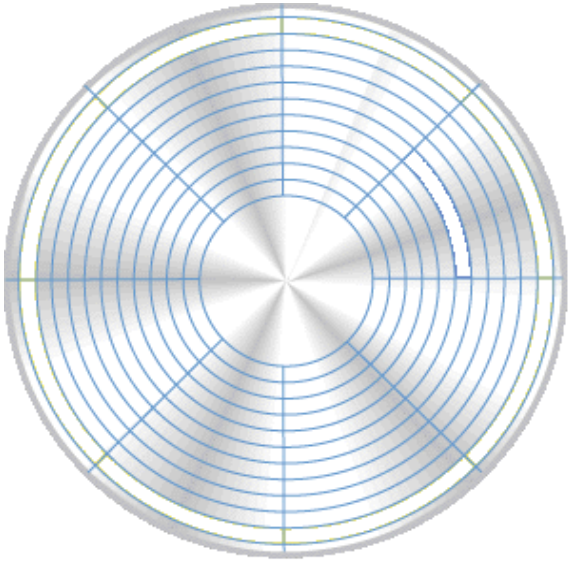
Hard Drives



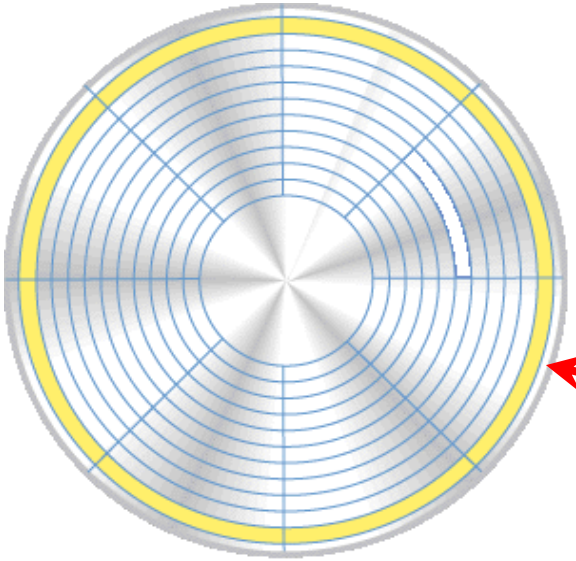
“Spindle”

(reads platter head)

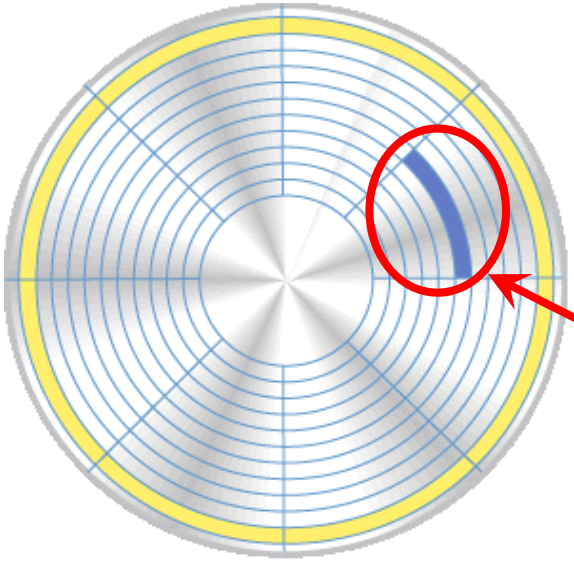
Photos from www.howstuffworks.com



Each platter has various components

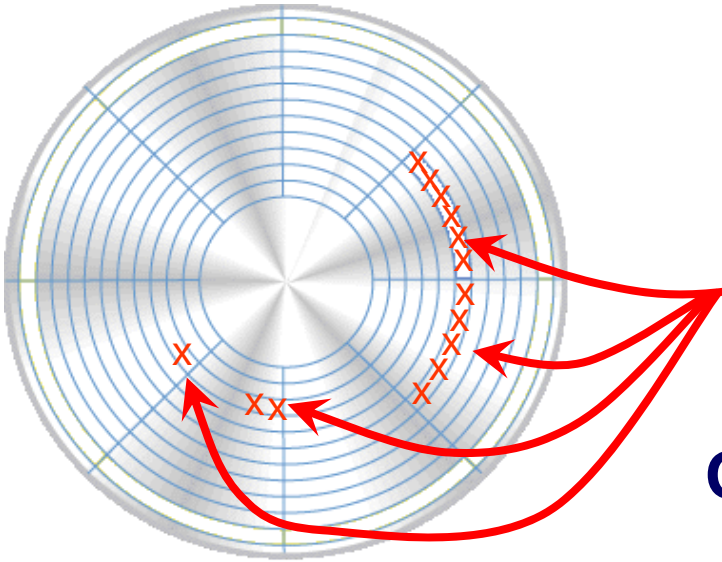


Platters have TRACKS



Platters also have

CLUSTERS



Files are written clusters

One file may take more or less than one cluster

One file may write to non-contiguous clusters

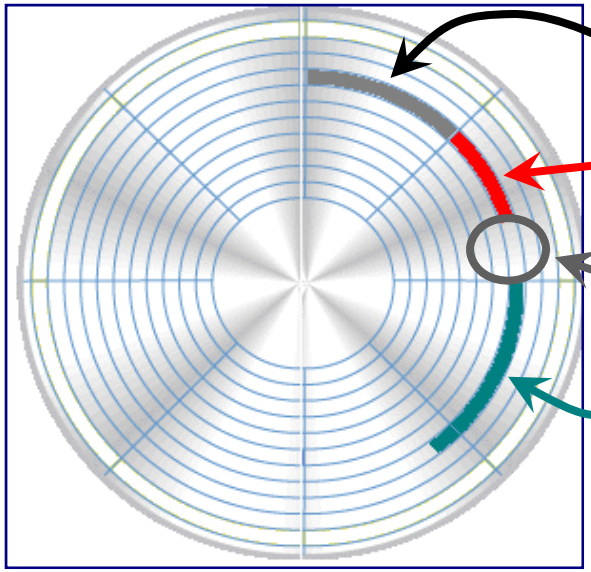
SLACK SPACE

- Area between the end of a file and the end of the last cluster or sector used by that file

UNALLOCATED / ”FREE” SPACE

- Clusters on a drive that are not currently assigned to a file

Slack Space



Unallocated space (unused)

File 1 stored in active file space.

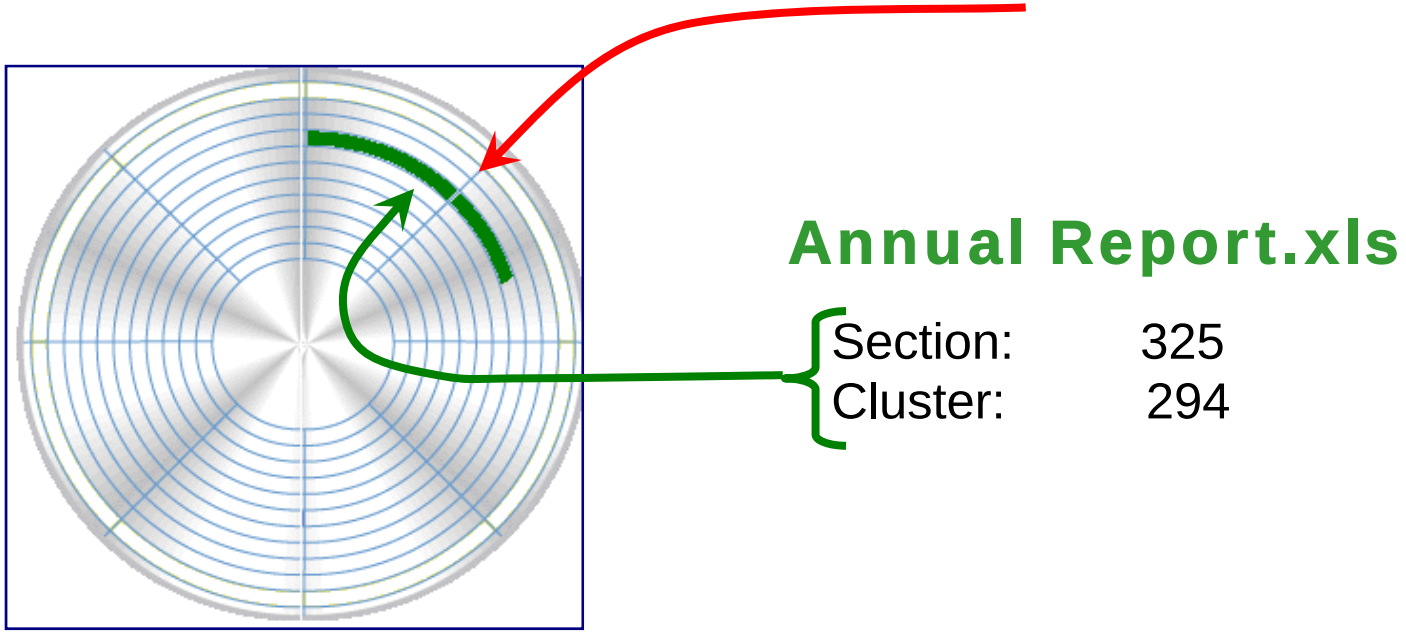
Slack space (end of cluster)

File 2 stored in active file space.

Deleted Files

- ✓**Deleted files create a special situation.**
- ✓**The term “deleted” does not reflect the actual situation.**
- ✓**The file itself is not deleted, only the index or “pointers” to that file.**

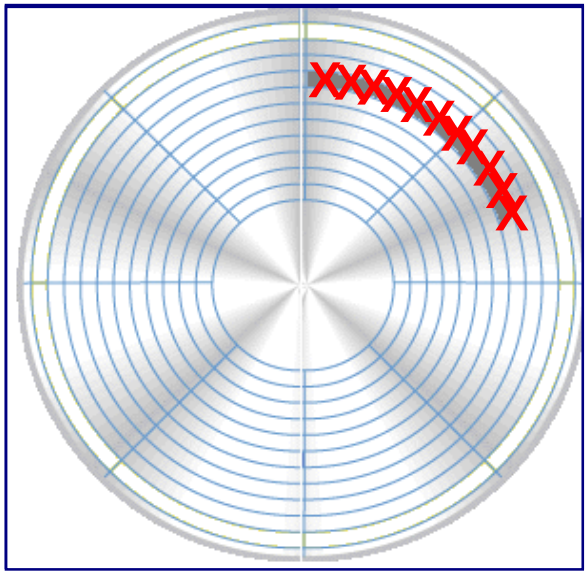
A file is written to the hard drive cluster(s).



A computer uses “pointers” to track where each file is located.

Deleted Files

A deleted file remains in the place it was originally.



~~Annual Report.xls~~

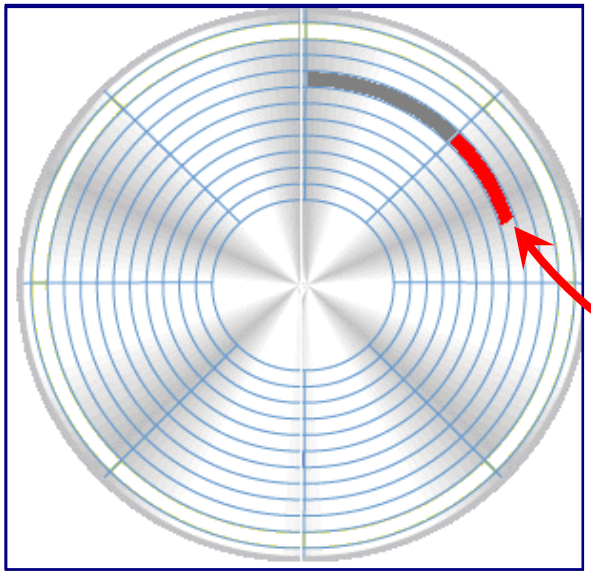
Only the computer "pointers" are ~~removed~~.

The actual file is still in place – the system just can't "find it".

The original space is now known as UNALLOCATED space.

Deleted Files

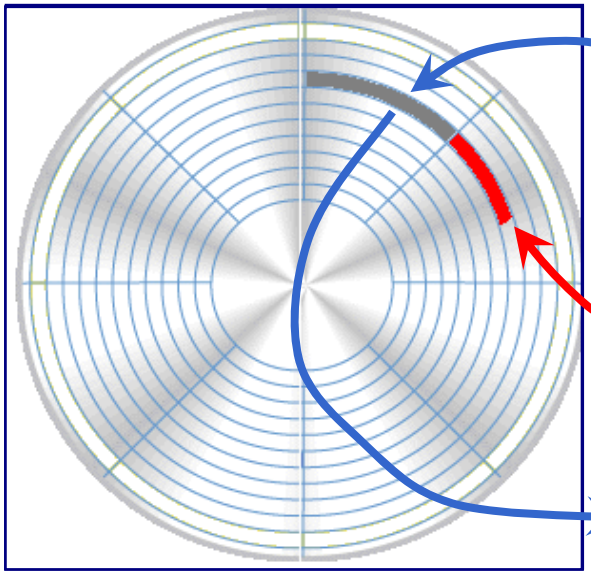
Other files can now be written in the unallocated space



The new files may take up less or more space than the original file.

Unallocated Space

Part or all of the previous file may be available for discovery.



Annual Report.xls

ABC Contract.doc

	Oct	Nov	Dec
Area 1	45,127	55,212	50,212
Area 2	27,444	32,617	*2 ~~~**
Total	**72,571**	**878***~	**50,212**

Not all the data within the file may be available to recover.

“HEXADECIMAL”

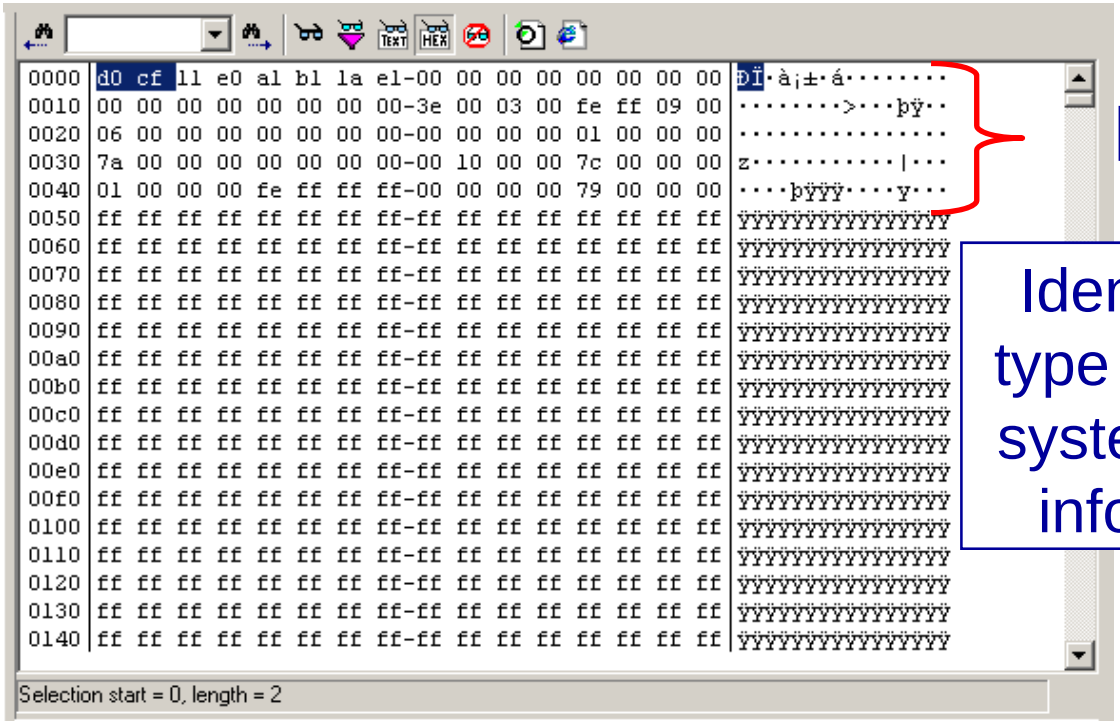
- Binary representation of data
- Base 16
  - 0 through 9
  - A through F

00a70	49	4e	43	4c	55	44	45	50	49	43	54	55	52	45	20	22	INCLUDEPICTURE "
00a80	68	74	74	70	3a	2f	2f	65	64	72	6d	2e	6e	65	74	2f	http://edrm.net/
00a90	69	6d	61	67	65	73	2f	61	2f	61	64	2f	45	64	72	6d	images/a/ad/Edrm
00aa0	5f	6f	76	65	72	76	69	65	77	2e	6a	70	67	22	20	5c	_overview.jpg" \
00ab0	2a	20	4d	45	52	47	45	46	4f	52	4d	41	54	49	4e	45	* MERGEFORMATINE
00ac0	54	20	14	01	15	15	0d	0d	4c	61	75	6e	63	68	65	64	T ·····Launched
00ad0	20	69	6e	20	4d	61	79	20	32	30	30	35	2c	20	74	68	in May 2005, th
00ae0	65	20	45	6c	65	63	74	72	6f	6e	69	63	20	44	69	73	e Electronic Dis
00af0	63	6f	76	65	72	79	20	52	65	66	65	72	65	6e	63	65	covery Reference
00b00	20	4d	6f	64	65	6c	20	28	45	44	52	4d	29	20	50	72	Model (EDRM) Pr
00b10	6f	6a	65	63	74	20	77	61	73	20	63	72	65	61	74	65	oject was create
00b20	64	20	74	6f	20	61	64	64	72	65	73	73	20	74	68	65	d to address the
00b30	20	6c	61	63	6b	20	6f	66	20	73	74	61	6e	64	61	72	lack of standar
00b40	64	73	20	61	6e	64	20	67	75	69	64	65	6c	69	6e	65	ds and guideline

“HEADER”

- Data placed at the beginning of a file
- How to handle that particular file
- Identifies key attributes of each file

Example of “header”



Header

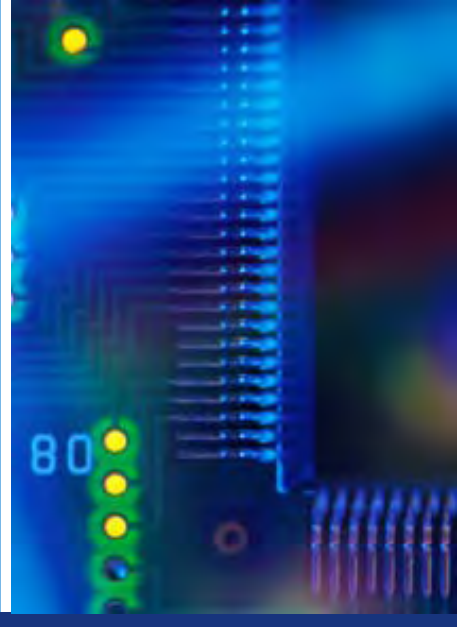
Identifies file type and other system critical information

Hexadecimal Representation

You also find evidence . . .

And you also find evidence in. . .

Sensing Diagnostic Module (SDM) – Car's Black Box



Electronic Discovery

METHODS USED TO REVIEW EVIDENCE or DATA EVIDENCE ANALYSIS

Done once the computer has been properly seized

Digital Evidence Analysis

There are 3 main steps to evidence analysis after you have seized a computer system:

- **Preservation**
  - » **protect the evidence from changing**
- **Duplication**
  - » **Create working copies so you don't change your evidence**
- **Investigation**
  - » **Searching for evidence.**

Digital Evidence Analysis

What tools are available to law enforcement to conduct such media analysis?

Phase	Objective	Tools
Preservation	• Protect Evidence • Create Image File	FTK SAFEBACK DISKIMAG
Duplication	• Prepare Media • Make Working Copy	RITEDISK SAFEBACK DISKMAK
Investigation	• Search Logical Structure • Search Residue • Search for text/non-text	FTK EnCase NORTON UTIL. CARVTHIS

Evidence Analysis

I. Print Review
II. Native Application Review
III. Legally Defensible Review
IV. Forensic

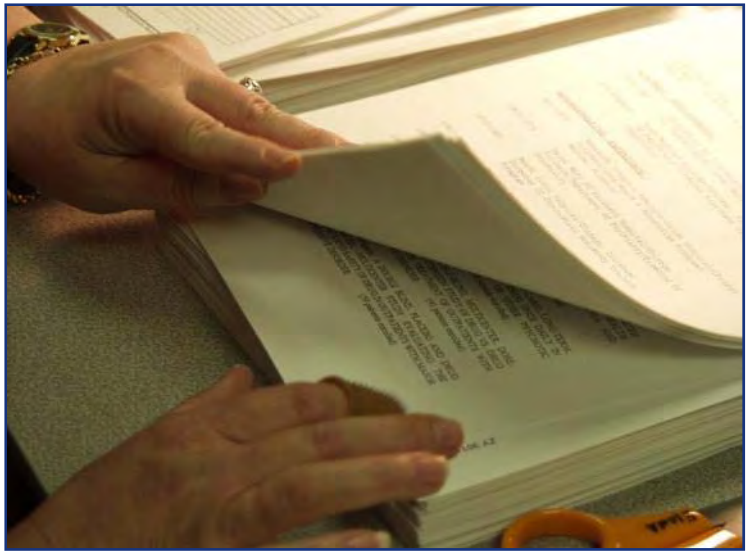
Print Review

Print emails and e-docs and data

Review in paper format

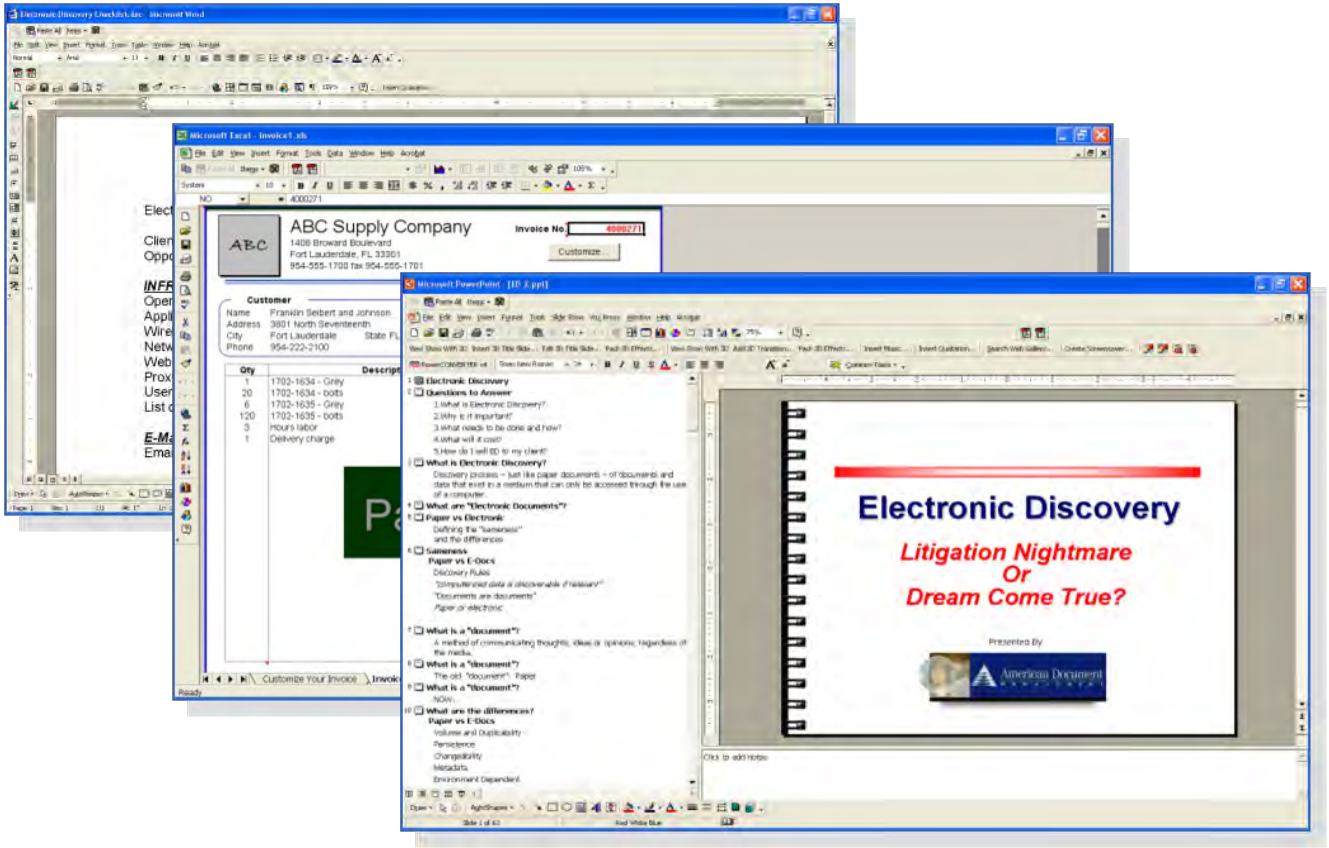
Very time consuming

Not efficient for examiner



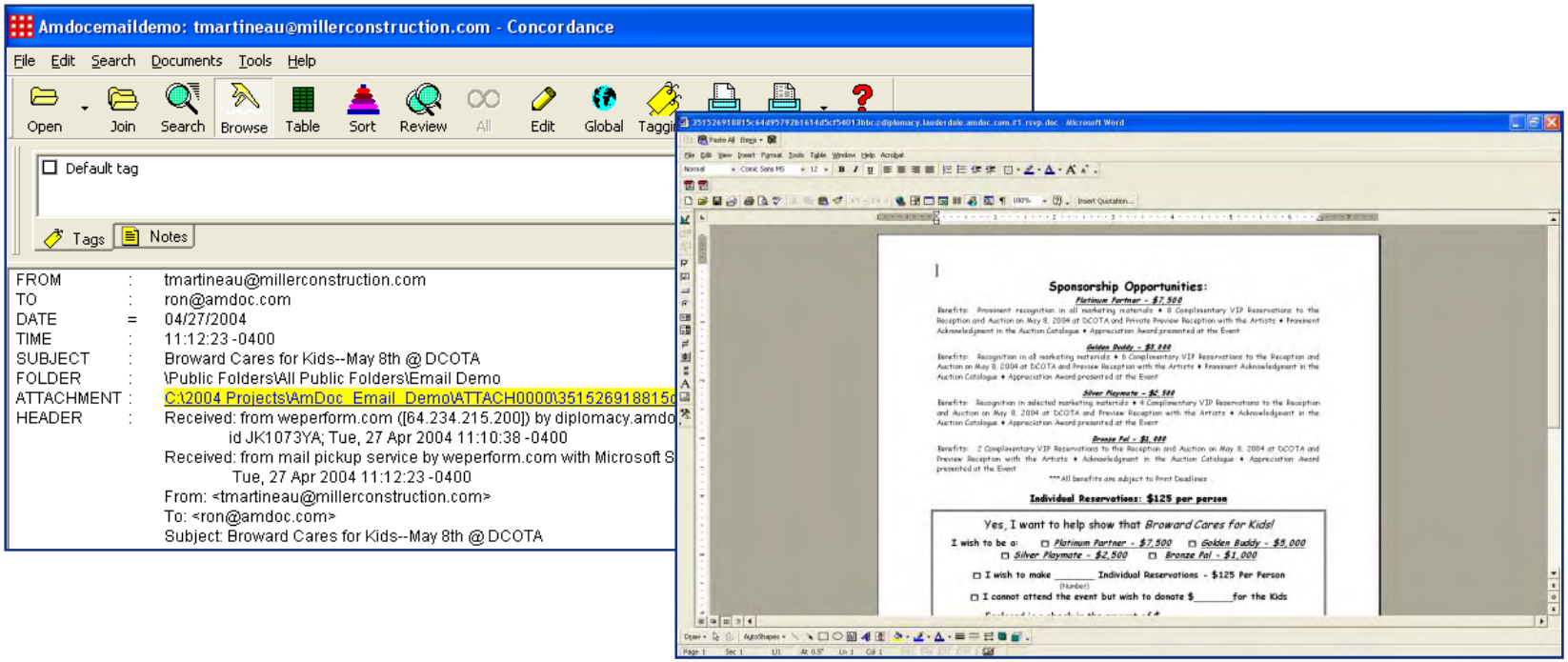
Native Application Review

Review documents within the program used to create



Software the Emulates Native File Review

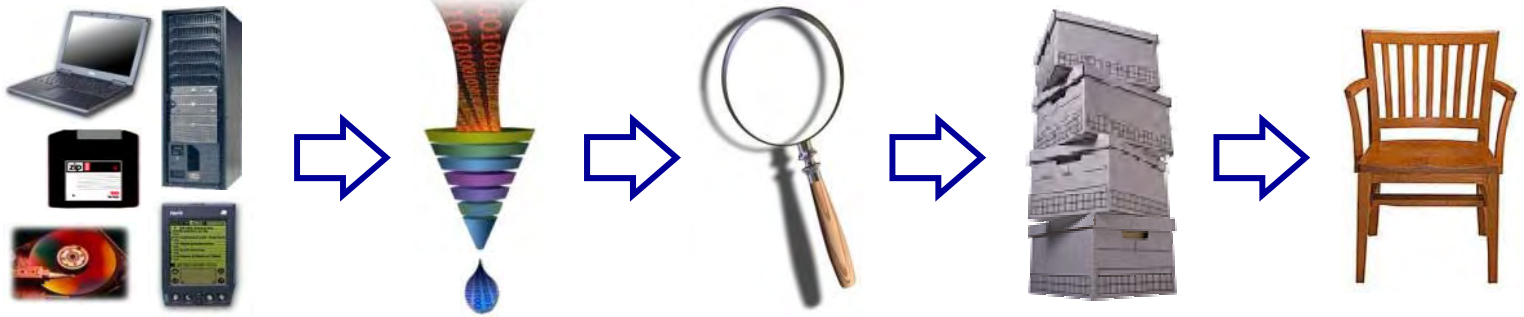
Use of forensic software to emulate view within native application



Forensic Level Data Recovery

- ✓ Expert capture
- ✓ Backup tapes
- ✓ Fragmented, erased or damaged files
- ✓ Sampling taken
- ✓ Clone (not copy) data
- ✓ Examine and recover data
- ✓ Decrypt encrypted files
- ✓ Convert to readable/searchable format
- ✓ Expert Witness Testimony

Forensic Data Recovery Process



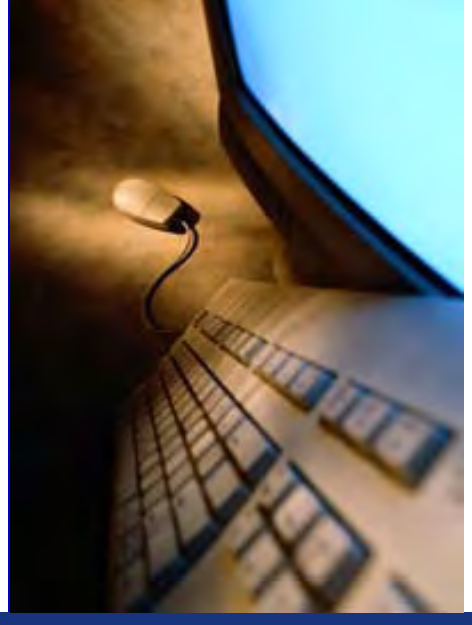
Evidence Collection

Evidence Processing

Evidence Review

Evidence Production

Expert Testimony



E-Forensics vs. Electronic Discovery

Definitions

Important Issues

Questions to Answer

Electronic Discovery

Electronic Discovery is the process, just like that for paper documents, of documents and data that exist in a medium that can only be accessed through the use of a computer.

Sedona Principles for Electronic Document Production

What **are** “Electronic Documents”?

Information created, stored and/or utilized using computer technology.

Federal Judiciary Counsel
Research Division

The NEW “Document”

Paper . . . . *PLUS*

- Word processing files
- Spreadsheets
- Email
- Presentations
- Databases
- Calendars & task lists
- Internet files
- Accounting files
- Handheld “Palm” files
- GIS drawings / maps
- Engineering documents
- CAD drawings
- Graphics files
- Voice mail
- Video clips / movies
- Tape recordings
- Video / PC games
- Instant message files
- Smart phones
- IPODs

Paper vs. Electronic Documents “What’s the Difference?”

- Volume
- Duplicability
- Persistence
- Changeability
- Environment Dependent
- Location Dynamic
- Search ability
- Metadata

“METADATA”

“Information About The Data”

- Varies by type of document (email, spreadsheet, etc.)
- Not all can be seen by user
- Hidden codes within application
  - Spreadsheet calculations
  - Internet “cookies” / search tags

Example of Metadata

	Word	PowerPoint	Excel
Document Name	✓	✓	✓
Title	✓	✓	✓
Author	✓	✓	✓
Company	✓	✓	✓
Creation date	✓	✓	✓
Last save time	✓	✓	✓
Last printed	✓		✓
Application name		✓	✓
Revision number		✓	
Last author			✓

Word

Last 10 Authors
Track Changes
White Font
Revision Number
Date Completed
Department
Graphics
Client

PowerPoint

Embedded Objects
Hidden Objects
Speaker Notes
Headers/Footers
Hidden slide(s)

Excel

Hidden Rows
Hidden Columns
Hidden Worksheet(s)
PivotTable Cache
Hidden Objects
Headers/Footers

WORKFLOW

- ✓ **Request “documents”**
- ✓ **Capture documents**
- ✓ **Inventory**

Virus Check

File Listing

Size and Type

Password Detection

CLIENT REVIEW

Client reviews report to determine “go” for processing

WORKFLOW

- ✓ Request “documents”
- ✓ Recover documents
- ✓ Inventory
- ✓ **Reduce documents**

FILTERS

- ✓ **Date**
- ✓ **Keywords**
- ✓ **Application Type**
- ✓ **Known File Types**
- ✓ **De-Dupe**
  - Custodian
  - Case
  - Job

WORKFLOW

- ✓ Request “documents”
- ✓ Recover documents
- ✓ Inventory
- ✓ Reduce documents
- ✓ **Extract and Load**

Extract metadata

Near Duplicate Identification

What’s “Near Duplicate Identification?”

LOAD TO RETRIEVAL SYSTEM

- *iConectNXT*
- *Summation*
- *Concordance*
- *IntroSpect*
- *And others . . .*

WORKFLOW

- ✓ Request “documents”
- ✓ Recover documents
- ✓ Inventory
- ✓ Reduce documents
- ✓ Extract and Load
- ✓ **Responsive Review**

Legal team reviews documents to determine *which* are responsive to request.

Strategy begins to form.

WORKFLOW

- ✓ Request “documents”
- ✓ Recover documents
- ✓ Inventory
- ✓ Reduce documents
- ✓ Extract and Load
- ✓ Responsive Review
- ✓ **Convert**

.PDF

.TIF .JPG

Responsive documents may be converted to image format and linked to the metadata and full text.

This allows:

- **Quicker review**
- **Redaction**
- **Annotations**
- **Tracking productions ***

* Depends upon retrieval system utilized

WORKFLOW

- ✓ Request “documents”
- ✓ Recover documents
- ✓ Inventory
- ✓ Reduce documents
- ✓ Extract and Load
- ✓ Responsive Review
- ✓ Convert
- ✓ **Additional Review**
  - Strategic
  - Redaction/Production

The legal team may choose to do additional reviews for updated information, strategic decisions and redaction prior to production.

Additional tools can be used like Concept Searching, Objective Auto-Coding or Subjective Coding.

Some retrieval systems will track productions automatically.

WORKFLOW

- ✓ **Request “documents”**
- ✓ **Capture documents**
- ✓ **Inventory**
- ✓ **Reduce documents**
- ✓ **Extract and Load**
- ✓ **Responsive Review**
- ✓ **Convert**
- ✓ **Additional Review**
  - Strategic
  - Redaction/Production
- ✓ **Production**

Produce documents for:
- Document Requests
- Depositions
- Trial

RECOMMENDED METHODOLOGY

Cost Effective Electronic Review Process

1. Identify key people and location of data
2. Capture deleted/unallocated, as needed (must request)
3. Determine file types to process via inventory
4. Reduce collection
5. Extract metadata, full text/OCR and native files For Review
6. Review for responsiveness, group by near-dupes
7. Convert ***ONLY*** files needed for Further review, Redaction and Production
8. Produce as needed

Significant Differences to Document Collections

- **Volume**
- **Size**
- **Duplicability**
- **Persistence**
- **Data Changes**
- **Environment-centric**
- **Dynamic locations**
- **Metadata / Deleted Files / Hidden Info**
- **Passwords**

REVIEW TECHNIQUES

OLD	NEW
X Paper review	✓ Scanned paper + electronic docs + email
X Objective Coding	✓ "Objective" Coding (opt) ✓ Auto-Coding

Contact Information:

- **Thomas Sadaka**
  Seiden Alder Matthewman & Bloch, PA

  Celebration Corporate Center
  1420 Celebration Blvd, Suite 201
  Celebration, Florida 34747
  407-566-2110
  E-mail: TSadaka@seidenlaw.com

  Boca Raton Coral Springs, Miami, Orlando